

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al.,
Plaintiffs,
v.
GOOGLE LLC,
Defendant.

Case No. 23-cv-02431-VC

**ORDER REQUESTING FURTHER
BRIEFING**

Re: Dkt. No. 164

The Court apologizes for the delay. This is a difficult case. The Court is very tentatively inclined to reach the following conclusions and requests that the parties file supplemental briefs addressing them:

1. One of the things that makes this case so tricky is the lack of a clear overlap between the conduct the plaintiffs complain about in this case and some of the statutes they invoke. As the Court understands it, this lawsuit is and always has been focused on Google’s receipt of private health information that can be linked to an identifiable person. Dkt. No. 159, Second Amend. Compl. ¶¶1, 21. But some of the statutory provisions invoked by the plaintiffs are broader—they cover the intentional interception of any communication without the consent of one party (or both parties) to the communication. It was probably a wise choice for the plaintiffs to focus their lawsuit in this fashion, but it makes it difficult to apply concepts like intent from statutes like the Federal Wiretap Act and CIPA (and from the case law interpreting those statutes). In any event, given the subject matter of the lawsuit, the focus here must be on whether the plaintiffs have adequately alleged that Google has obtained their private health information in a way that enables Google to actually identify them and link the information to them.

2. On the Court's current understanding of the allegations in the SAC and related documents, the products at issue here work as follows: The health providers decide which Google products they would like on their webpages and configure those products according to their preferences. One way those products can collect information is by using cookies. Cookies collect certain pieces of information that are then sent to Google and the health providers. Those data can then be used by the health providers to determine how users interact with their websites. The data transmitted by the cookies might not always, or even usually, contain health information, but depending on what is collected by the cookies, material that could be considered health information may be transmitted via the cookies on a specific webpage. *See, e.g.*, Dkt. No. 159-4 at 5 (appearing to send information that a specific user ID attempted to book an appointment with a specific doctor).

At least one cookie—the gid cookie—seems to collect information that, when a website interaction involves Google account holders, can link that website interaction to those account holders in a way that identifies them. The plaintiffs allege that this cookie generates and then transmits a unique identifier assigned to a website user when that user is logged into a Google service on the same browser. The plaintiffs further allege that this identifier can be tied to that user's Google account. Based on this, it appears reasonable to infer that Google, which obviously knows the personal information that users input to create their Google accounts, can use the gid cookie to tie information that came from the health providers' webpages to a specific person. On the Court's understanding, when a specific action happens on a webpage with these cookies enabled, there will be several types of cookies that contain different data. Some of those cookies may end up sending health information, and when that transmission also includes the gid cookie with a specific gid identifier attached, Google is collecting health information about a particular, identifiable Google account holder. The plaintiffs allege that this health information then becomes included in Google's "digital dossier" on that person. If this cannot be inferred from the allegations in the SAC, Google should explain why, with reference to the SAC and materials that can properly be considered at this stage.

By contrast, the plaintiffs do not appear to have adequately alleged that Google collects private health information on non-Google account holders that can be linked to them in an identifiable way. In contrast to the gid cookie, the cid cookie seems to be a synonymized cookie, i.e., one that is assigned to a particular user but does not collect any information that could be used to identify a person in the real world. For example, on the Court’s understanding, the data package connected to a particular cid identifier would look something like this: the user or browser that has been assigned this particular cid identifier has looked at information about the Kansas City Chiefs, shops at Banana Republic, and has searched for “anxiety” and “bill pay” on the Gunderson Health website. What the plaintiffs seem to be missing is an allegation that Google is able to tie the cid cookie to any personally identifying information. To the extent that information is in the SAC, where is it, and if there are inferences that must be drawn to determine that Google is able to make information connected to the cid cookie personally identifiable, what are those inferences?

3. Breach of Contract: For the reasons discussed above, it appears that the plaintiffs may have stated a claim based on allegations that Google collected communications about private health information between patients and providers that could be linked to Google account holders through the cookies tied to users’ accounts, after promising to collect only health information that Google account holders chose to provide. *See* Second Amend. Compl. ¶¶ 96–101; Dkt. No. 159-4 at 5; Dkt. No. 159-5. It appears that a reasonable person reading Google’s Privacy Policy could conclude that Google promised to only collect health information after consent by users and that the health information at issue here was covered by that promise. Dkt. No. 158-14 at 19.

4. Intent: The Federal Wiretap Act applies when a person “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511. The intent element of the Federal Wiretap Act requires a defendant to act “purposefully and deliberately and not as a result of accident or mistake.” *United States v. Christensen*, 828 F.3d 763, 774 (9th Cir. 2015). Although

no “evil” motive is required, the defendant must have “acted consciously and deliberately with the goal of intercepting wire communications.” *Id.* at 774.

Section 631 of CIPA applies when someone “willfully and without the consent of all parties to the communication . . . reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit.” Cal. Penal Code § 631. The intent inquiry under section 631 is identical to the intent inquiry under the Federal Wiretap Act. *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1079 (N.D. Cal. 2023), *motion to certify appeal denied*, No. 22-CV-03580-WHO, 2024 WL 4375776 (N.D. Cal. Oct. 2, 2024) (“Intent under CIPA is determined consistently with intent under ECPA.”).¹

As mentioned at the outset, this lawsuit seeks to hold Google liable for intercepting communications about private health information that Google can link to a particular, identifiable individual. Therefore, it doesn’t matter (at least for purposes of this lawsuit) whether Google intended to intercept other types of communications. If Google intended to intercept communications that contained no private health information, that wouldn’t matter. And even if Google intended to intercept communications about private health information (which it denies), that wouldn’t matter for purposes of this suit if Google couldn’t link the information to a particular, identifiable person.

The plaintiffs may indeed have adequately alleged that Google, prior to publication of its 2023 HIPAA disclosure, intended to receive private health information that it could link to individual Google account holders. We know, of course, that Google intended to receive communications between website visitors to health provider pages and health providers

¹ For section 632, the intent inquiry is narrower and centers on whether the person intended to record a *confidential* communication. *See Rojas v. HSBC Card Services Inc.*, 20 Cal. App. 5th 427, 434–35 (2018) (“[I]t is not the purpose of the statute to punish a person who intends to make a recording but only a person who intends to make a recording of a confidential communication.” (quoting *People v. Superior Court of Los Angeles County*, 70 Cal. 2d 123, 133 (1969))). But that inquiry would likely be the same as the inquiry under the Federal Wiretap Act and section 631 (at least at this stage) given the allegations offered as to Google’s intent to collect personal health information.

generally. It was obvious that some of these communications would be between patients and providers; it therefore was obvious that some of them would disclose private health information. Thus, unless Google took some measure to prevent itself from receiving communications about private health information and/or took some measure to prevent itself from being able to link those communications to an identifiable Google account holder, it would be reasonable to infer that Google intended to receive communications between patient and provider that were linkable to an identifiable Google account holder. In light of the plaintiffs' allegations about the gid cookie, and in light of the allegation (based on the 2018 HIPAA disclosure) that Google did not explain to providers how to avoid sharing private health information about identifiable Google account holders through the gid cookie, it's plausible to infer that Google intended to receive these communications. The Court is somewhat skeptical that the plaintiffs will be able to prove that at the end of the day, but it seems like it could be a reasonable inference to be drawn from the allegations in the SAC and the supporting documents.

In contrast, following Google's new HIPAA disclosure in 2023, it would not be reasonable to infer from the allegations in the SAC that Google intended to receive personal health information that could be linked to identifiable Google account holders. In that disclosure, Google told providers not to use Google's products on any page that may be related to the provision of health care services and are likely to be covered by HIPAA. This, as the Court understands it, would prevent the gid cookie from sending personal health information in a way that would allow Google to link it to identifiable Google account holders because the cookie would not be on any page containing personal health information. Although at times the plaintiffs seem to suggest that the new 2023 disclosure was just part of a plot by Google to keep getting the type of health information that is the focus of this lawsuit, that allegation would be governed by Rule 9(b), and the plaintiffs have not come close to satisfying the Rule 9(b) standard. Indeed, as mentioned above, it seems questionable that the plaintiffs will be able to prove that Google intended to receive these types of communications even before 2023.


Google's primary job in its supplemental brief, then, is to explain why the above analysis

is wrong as it relates to the pre-2023 period. The plaintiffs' primary job is to explain why it's right, although they are free also to try to explain why the Court is wrong as to people who don't have Google accounts, or as to Google's post-2023 HIPAA disclosure conduct with respect to people who do have Google accounts.

Google's brief should be filed no later than 7 days from this order, the plaintiff's response should be filed no later than 14 days from this order, and Google may reply no later than 21 days from this order. The parties' initial submissions should not exceed fifteen pages, and Google's reply should not exceed 10 pages.

IT IS SO ORDERED.

Dated: March 20, 2025



VINCE CHHABRIA
United States District Judge